Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of protecting a victim site against a denial of service attack, the method comprises:

~~receiving network packets with faked source addresses;~~

receiving from the victim site a notification that the victim site is under an attack; and

sending queries to data collectors, deployed at different points in a network that carries network traffic to the victim site, that sample network packets and collect statistical information on network packets sent over the network, to request the statistical information from at least some of the data collectors, the statistical information to determine the source of suspicious network traffic ~~being~~ sent to the victim data center.

2. (Currently Amended) The method of claim 1 wherein the network packets from the attacker have faked, random source addresses that change with time, and sending queries further comprises:

sending queries to the data collectors for the statistical information based on victim destination address.

3. (Currently Amended) The method of claim 1 wherein based on collected statistical information the method further comprises:

determining what data centers are performing the spoofing on the victim.

4. (Original) The method of claim 3 wherein determining is performed by a control center, and determining further comprising:

sending data to/from a gateway device that is associated with the victim center.

5. (Original) The method of claim 4 wherein the gateway identifies the network address of the victim, via a message to the control center.

6. (Original) The method of claim 5 wherein the message is sent over a hardened network.

7. (Original) The method of claim 5 wherein message indicates the type of attack.

8. (Original) The method of claim 1 wherein the attacker is behind a gateway.

9. (Original) The method of claim 8 wherein if the attacker is behind a gateway, the control center issues a request to the gateway that the attacker is behind to block the attacking traffic.

10. (Original) The method of claim 8 wherein if the attacker is behind a gateway, the gateway that the attacker is behind selectively discards traffic that appears to be malicious traffic and that contains the victim destination address.

11. (Original) The method of claim 1 wherein if the attacker is not behind a gateway, the control center queries the data collectors to provide information about possible locations of the attackers.

12. (Original) The method of claim 1 wherein if the attacker is not behind a gateway, the method further comprises:

contacting administrators at locations involved in attack to have the administrators take action to filter out packets with the destination address.

13. (Original) The method of claim 1 wherein the attack is a low-grade spoofing-type of attack that does not compromise network traffic flow between the victim data center and Internet.

14. (Original) The method of claim 1 wherein the attack is a high-grade attack that compromises network traffic flow between the victim data center and Internet.

15. (Currently Amended) A method of protecting a victim site against a denial of service attack, the method comprises:

receiving packets with faked, random source addresses;

receiving, from a gateway disposed near the victim site, a notification that the victim data center is under an attack, ~~from a gateway disposed near the victim site~~;

sending queries to data collectors, deployed at different points in a network that carries network traffic to the victim site, that sample network packets and collect statistical information on network packets sent over the network to request statistical information from data collectors that have examined network traffic with the victim destination address; and

determining the data center or centers involved in the attack on the victim by analyzing collected statistical information from the data collectors.

16. (Original) The method of claim 15 wherein the control center also includes a communication process to send data to/from a gateway device that is disposed with the victim center.

17. (Original) The method of claim 16 wherein if the attacker is behind a gateway, the control center issues a request to the gateway to block the attacking traffic.

18. (Original) The method of claim 17 wherein if the attacker is behind a gateway, the gateway selectively discards traffic that appears to be malicious traffic and that contains the victim destination address.

19. (Original) The method of claim 15 wherein if the attacker is not behind a gateway, the method comprises:

contacting administrators at locations involved in attack to filter out packets having the destination address.

20. (Currently Amended) A system to thwart denial of service attacks on a victim data center, the system comprising, ~~comprises~~:

a plurality of monitors dispersed throughout a network, the monitors collecting statistical data on network traffic;

a control center coupled to the plurality of data collectors, the control center executing a computer program product stored on a computer readable medium, comprising instructions for causing a computer to:

receive from the victim site a notification that the victim data center is under an attack; and

send queries to data collectors to request information from data collectors, the information used to determine the source of suspicious network traffic being sent to the victim;

a gateway device that passes network packets between the network and the victim site, the gateway disposed to protect the victim site, and being coupled to the control center.

21. (New) The system of claim 20 wherein the data collectors collect statistical information on network packets that pass through points in the network that the data collectors monitor.

22. (New) The system of claim 20 wherein the control center further comprises instructions to:

determine the source of the attack on the victim data center by analyzing collected statistical information from the data collectors.

23. (New) The system of claim 20 wherein the control center and gateway device associated with the victim center exchange data to thwart the attack.

24. (New) The system of claim 20 wherein data exchanged between the control center and gateway device associated with the victim center are sent over a redundant network that is a different network than the network that is being monitored by the data collectors.

25. (New) The system of claim 20 wherein if the control center determines that the attacker is behind a gateway, the control center issues a request to the gateway that the attacker is behind to block the attacking traffic.

26. (New) The system of claim 20 wherein if the control center determines that the attacker is behind a gateway, the control center issues a request to the gateway to selectively discard traffic that contains the victim destination address.

27. (New) The system of claim 20 wherein if the attacker is not behind a gateway, the control center queries the data collectors to provide information about possible locations of the attacker.

28. (New) The system of claim 27 wherein if the attacker is not behind a gateway, the system includes instructions to contact administrators at locations involved in attack to have the administrators take action to filter out packets with the victim destination address.

29. (New) A computer program product residing on a computer readable media for protecting a victim site against a denial of service attack, the computer program product, comprising instructions for causing a computing device to:

receive a notification that the victim data center is under an attack;

send queries to data collectors, deployed at different points in a network that carries network traffic to the victim site and that sample network traffic and collect statistical information on packets sent over the network, to request statistical information from data collectors that have examined network traffic with the victim destination address; and

determine a source of the attack on the victim by analyzing collected information from the data collectors.

30. (New) The computer program product of claim 29 further comprising instructions to:

send data between a gateway device that is disposed with the victim center and a control center.

31. (New) The computer program product of claim 29 further comprising instructions to:

determine whether the attacker is behind a gateway and if the attacker is behind a gateway,

issue a request to the gateway to block the attacking traffic.

32. (New) The computer program product of claim 29 further comprising instructions to:

determine whether the attacker is behind a gateway and if the attacker is not behind a gateway,

send a message to contact administrators at locations involved in attack to filter out packets having the destination address.